PROCYON PARTNERS

Cybersecurity for Plan Sponsors:

What You Need to Know and What Actions to Take

Today, it is hardly surprising that the term "cybersecurity" is ubiquitous as the issue that regularly makes news headlines around the world.

Indeed, it is a complex and rapidly evolving area in which plan sponsors need to be both vigilant and conversant in order to protect the interests and sensitive information of their overall business and plan members. Before we explore the key risks of inadequate cybersecurity and the responsibility of plan sponsors to protect participants against such risks, it's instructive to define the term.

According to the definition put forward by the global cyber-security firm Kapersky Lab, "cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks."[1]

Nobody is immune to the threat and potential harm of sophisticated cybercrime. Financial institutions (banks, online brokerages, credit card companies, etc.), social media networks, online/traditional retailers and other ecommerce sites, government bodies and academic institutions are all prime targets for cybercrime, as are others who depend on reliable, secure data flow of sensitive information.

Example: Equifax Inc.

For example, one notable case of a cybersecurity breach involved Equifax Inc., a major U.S.-based consumer credit reporting agency. In September 2017, its systems had been breached by hackers. The names, home addresses, social security numbers and other personal information of roughly 148 million Americans had been compromised. Many consumers also had their credit card numbers exposed as a result of the cyberattack. The broad scope of this security breach and the extent of sensitive personal information involved made the Equifax breach unprecedented. Other noteworthy breaches across industries and countries have since followed.[2]

[1] Kaspersky Lab, *What is Cyber-Security?*
[2] Epic.org, *Equifax Data Breach*

With new cyber risks constantly emerging to endanger the integrity of electronic information, it's not surprising that financial services firms are expected to continue ramping up cybersecurity spending, which may reach US$43 billion globally by 2023.[3]

CYBERCRIME: Hard to pinpoint a single motivation

There are many reasons for individuals or organizations to commit cybercrime, including the following:

- They may want to misappropriate sensitive personal information to commit fraud for financial gain.
- They may seek the intellectual challenge, wanting to showcase their technological skills and "earn" notoriety for exposing an organization.
- They may have a vendetta against an organization and want to compromise important data. Their main goal is to inflict reputational damage and highlight an organization's technological vulnerability.

Cybersecurity: Plan sponsor challenges and risks

What does cybersecurity mean for plan sponsors? First and foremost, cybersecurity should be an integral component of a plan sponsor's fiduciary duty. Fiduciaries to retirement plans have a legal obligation to act in the best interests of the plan participants, which includes protecting plan members' information just as much as it includes helping them structure a plan that will help them achieve a viable retirement.

A major cyber risk for plan sponsors in the normal course of their business as well as while administering retirement and benefit plans is the required management and sharing of sensitive employee and stakeholder data and asset information with third party vendors. Vendor firms have recognized the importance of cybersecurity and continue to invest heavily on information security. However, vendors are often reluctant to partner with plan sponsors – or even discuss specific details –regarding information security processes because the two entities are unrelated and any sharing could leave them exposed to another perilous layer of cyber risk. Therefore, it's incumbent on plan sponsors to undertake their own cybersecurity initiatives as part of a comprehensive, coordinated effort to protect employees and their personal data.

What are common cybersecurity threats?

Any activity that serves to put electronic data at risk may be considered a cybersecurity threat. The American Institute of Certified Professional Accountants (AICPA) has identified three key groups of information toward which cybercriminals would typically gravitate:

- Personally identifiable information, such as a social security number or credit card number
- Participant enrollment data, such as account balances and direct deposit information
- Electronic protected health information, such as health care status and provisions

In an effort to gain access to these types of private information, cyber criminals will often undertake the following illegal hacking activities:

- **Phishing.** This activity is "the fraudulent attempt to obtain sensitive information, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication."[4]
- **Malware on fake (malicious) website.** A malicious website is a site that may look completely legitimate, but attempts to install malware (something that will disrupt computer operation, gather your personal information or gain total access to your machine) onto your electronic device.[5]

[3] InvestmentNews, *Cybersecurity poses strain between plan sponsors, record keepers,* Mar 23, 2019
[4] Wikipedia, *Phishing*
[5] Norton, by Symantec, *Malware 101*

- **Using employee info to set up accounts.** Once cybercriminals have set up a fraudulent account, they can attempt to use these fake accounts to access a legitimate account (e.g., a 401(k) or other retirement account), open a credit card account, procure a loan or line of credit, or any number of other illegal activities that may have dire financial consequences for the unsuspecting employee.
- **Ransomware attacks.** Ransomware is a highly dangerous form of malware that threatens to publish the victim's data or blocks access to this data or other electronic functionality, unless some type of financial transaction (a "ransom") is carried out. Cybercriminals typically extort money from the victim using electronic means that are difficult to trace, such as wire transfers or digital currencies.
- **Drive-by downloads.** Through malware on a legitimate website or detachable drive, a program is downloaded to a user's system just by visiting the site or connecting to the target's system. Typically, a small snippet of code is downloaded to the user's system and that code then reaches out to another computer to obtain the rest of the program. A drive-by download often exploits vulnerabilities in the user's operating system or in other related programs.[6]

Bear in mind that all of the cyberbreaches discussed above are serious offences that may cause significant damage. Not only are there potential fines for fiduciaries such as plan sponsors if they fail to implement adequate cybersecurity measures to protect the plan members, but the negative publicity related to any data breach may cause irreparable damage to the plan sponsor's reputation.

By the numbers – personal data is at risk:[7]

6.4 billion	**Fake emails sent every day**
1.9 billion	**Pieces of sensitive information compromised (between January 2017 and May 2018)**
US$3.62 million	**The average cost of a data breach in 2017**
87%	**Organizations that lack sufficient budget to reach their desired levels of cybersecurity**
77%	**Organizations that are operating with limited cybersecurity resources**

Putting cybersecurity plans into action

The Department of Labor's (DOL) Advisory Council on Employee Welfare and Pension Plans has identified several universal considerations for plan sponsors as they develop their cybersecurity strategies, including:

Establishing the individuals or teams responsible for designing, documenting, implementing and maintaining the strategy

Creating an optimized process for **eliminating unnecessary data** to reduce the risk of cybercrime

Evaluating third-party service provider security programs and **documenting which sensitive data** they may access to and how they will gain access to this data

Understanding current insurance coverage arrangements to **determine if additional protection is needed** to adequately safeguard the plan sponsor and its participants

[6] Timothy Rouse, David Levine, Allison Itami and Benjamin Taylor, *Benefit Plan Cybersecurity Considerations: A Recordkeeper and Plan Perspective,* December 2018
[7] EY, Paul van Kessel, *Is cybersecurity about more than protection?* October 10, 2018

According to BDO, which offers public accounting, tax, consulting and business advisory services, the following actions may be pursued to build on the DOL's outlined recommendations and a practical first step of a plan sponsor's cybersecurity efforts (note that these recommendations are just as beneficial to a firms main business):[8]

- **Identify what information** you manage that could be at risk.
- **Monitor what service providers** are doing to address and mitigate risks at their organizations.
- **Review existing frameworks** and current industry developments through resources provided by the AICPA, SPARK Institute, DOL and other organizations.
- **Review the AICPA's System and Organization Controls** (SOC) for Cybersecurity and ask service providers if they have adopted those recognized practices.
- **Understand your organization's broader cybersecurity plan** and identify ways to tailor it in order to address the distinct risks that your retirement plans and participants face.

It can be challenging to identify all of a plan sponsor's cybersecurity responsibilities. Given the current absence of definitive guidance by regulatory bodies, there is no comprehensive cybersecurity regulatory framework that plan sponsors are obligated to follow. As a result, plan sponsors must be proactive to ensure that they have the necessary cybersecurity measures in place. Since each plan sponsor's situation and plan members' circumstances are unique, it's important for individual plan sponsors to develop and implement a customized cybersecurity plan to meet all of their specific needs.

This cybersecurity plan must be holistic in approach and complex enough to address the equally complex risks that cyber criminals may create for plan sponsors. An effective and vigilant cybersecurity policy needs to be coordinated across departments, given that cybersecurity threats often emerge in the periphery, such as during a seemingly innocuous activity like a phone call. Once the initial contact and point of entry have been made, the threat then moves inward in the direction of sensitive data and critical business functions. Clearly, it doesn't take much to initialize the cyberbreach process and have its damaging effects broaden and intensify.

Here are four of the crucial areas that an effective cybersecurity policy must cover:

Technology management. Aside from the baseline requirements – being able to defend against phishing, malware and ransomware, and being able to encrypt sensitive information and data – the technology you manage must be cost effective, scalable, compatible with third-party cybersecurity technology and efficient at data-loss prevention and authentication measures, while also offering the latest capabilities in overall network protection.

Data management. One of the most effective ways to implement the sound management of data is to limit who can access data and limit what type of data these individuals can share, store and retain. The smaller the circle of people who access sensitive data on an as-needed basis and the less volume of data transmitted, the lower the possibility of cyberbreaches.

Vendor relations. A third-party vendor's cybersecurity process can complement a plan sponsor's efforts, but on the other hand a vendor can also pose an added risk. To ensure that a vendor's impact on cybersecurity is positive, you should identify all service providers who access data in any way, and then understand each vendor's security procedures and whether they've been independently audited for effectiveness. Also note if these vendors outsource any activities to other providers; if yes, those outsourced providers must disclose their practices and meet your security requirements as well.

Training and education. Implementing effective cybersecurity ultimately boils down to equipping your technology experts with sufficient training and education. A key component of a strong cybersecurity strategy involves training all staff who are directly involved in benefit plans or have some form of access to plan data (including transmission and storage), and teaching them industry best practices. This training must stay updated as cybercrime evolves constantly and any educational efforts can quickly become obsolete.

[8] BDO, *Retirement Plan Sponsors: Is Cybersecurity Part Of Your Fiduciary Duty?* July 2018

Establish a risk management process

As noted, every plan sponsor will have different needs and different sets of sensitive data that may be vulnerable to cyberattacks. Your risk management process will begin with identifying which particular data is of concern from a cybersecurity perspective. Your process should be customized to recognize your greatest risks, specific resources available and security budget allocated.

Plan sponsors need to choose a cybersecurity risk management framework that is appropriate for their organizations. The National Institute of Standards and Technology (NIST), AICPA's SOC for Cybersecurity, the SPARK Institute's Best Practices for Recordkeepers are all good examples of policy frameworks that provide computer security guidance for assessing and improving the prevention and detection of cyberthreats, and often share best practices for responding to cyberattacks.

Plan sponsors also need to communicate openly on cybersecurity issues, educating employees and other participants on cyberthreats and what actions the plan sponsor is taking to address these serious issues. As an example, employees, clients, vendors and other stakeholders should be made aware of the reasons why they are being subjected to an enhanced (and often stringent) security verification process. While a lengthier login process may appear to be a nuisance, you should educate these individuals on why such measures are needed to protect them and the data they access. For employees, plan sponsors should provide regular educational updates on cybersecurity, and periodic phishing tests should be administered to identify internal deficiencies and vulnerabilities.

From an external standpoint, update your vendor relationships as needed and ensure that any contracts with vendors sufficiently address cybersecurity, including which individuals have access to what information. Streamline the chain of access as much as practicality will permit and eliminate inessential movement of sensitive data. You should also regularly conduct assessments and monitoring of vendor performance (including formal independent audits) to determine if any security processes need revising to satisfy your established standards.

Also consider a cyber insurance policy to help protect you against the unwanted and potentially significant consequences of future security breaches. Cyber insurance may help recover costs that a company incurs while addressing a cyberthreat, pay for fees and damages arising from cybercrime litigation, and reimburse for revenue lost or additional expenses incurred as a result of a cyber-related business disruption.

Fighting cybercrime through enhanced privacy rights

Government bodies are also trying to curb cybercrime and better protect the public. For instance, the California Consumer Privacy Act (CCPA), slated to become law on January 1, 2020, is intended to strengthen the privacy rights of California residents and offer enhanced consumer protection. It will allow residents to know what personal data is being collected and provides some legal recourse for those who do not want certain personal data collected, disclosed or sold.

The future is now for cybersecurity

Cybersecurity is a crucial and growing part of a plan sponsor's fiduciary duty. Having a comprehensive cybersecurity plan has become a necessity of business and not just an option to consider.

Yes, cybersecurity can be costly and complex. It requires the investment of significant time and resources to properly devise, implement and maintain a robust cybersecurity framework. However, not only can a robust process protect your sensitive data and the private information of your entire business and your plan members, it can also be an engine for your firm's future growth if the plan is able to function efficiently and effectively.

Procyon Partners is always looking for tangible ways to add value for our clients. We're pleased to provide this educational piece on cybersecurity so you can understand and address critical issues for you and your plan participants.

Cybersecurity learning center

For a basic primer on the cybersecurity issues and threats for retirement plan sponsors, read Is Cybersecurity Part of Your Fiduciary Duty?

The Department of Labor's Advisory Council on Employee Welfare and Pension Plans' Cybersecurity Considerations for Benefit Plans provides a detailed report on cyberthreats that are specific to retirement plans and plan sponsors.

For more information about cyberthreats and what plan sponsors can do about them, read Cybersecurity and employee benefit plans: Questions and answers, published by the American Institute of Certified Professional Accountants.

One of the challenges of implementing cybersecurity is the potential friction between plan sponsors and third-party vendors like record keepers. Gain insights into this thorny but often under-the-radar issue by reading Cybersecurity poses strain between plan sponsors, record keepers and also Retirement Plan Cybersecurity Disclosure to Make Everyone Satisfied.

To learn more about guidance and potential solutions regarding cybersecurity for benefit plans, read the December 2018 Pension Research Council Working Paper Benefit Plan Cybersecurity Considerations: A Recordkeeper and Plan Perspective.

Call (844) PROCYON today

Do you need alternative options for your retirement plan? Contact us to learn more about how Procyon can help you address the cybersecurity risks associated with your retirement plan.

PROCYON PARTNERS

One Corporate Drive • Suite 225 • Shelton, CT 06484 | (844) PROCYON | www.procyonpartners.net